الجامعة السعودية الالكترونية
Saudi Electronic University

COLLEGE OF COMPUTING AND INFORMATICS

Course Title : Operating System **Course Code : IT-241**

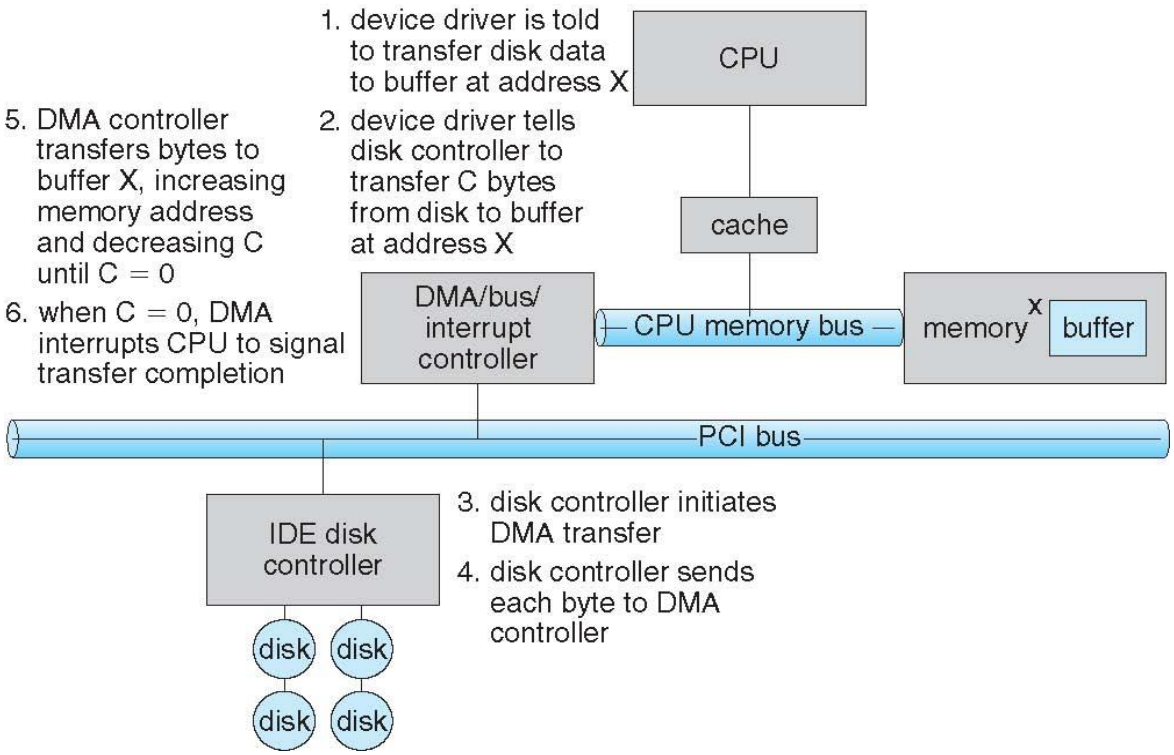
Assignment : 4

- **Answer all questions.**
- **All are asked to submit the assignment on or before 4 May 2016 at 11:59 pm.**
- **Total marks for this assignment are 5.**
- **Copied assignment will be graded zero.**
- **This assignment covers Chapter 13, 14, 15, 17.**

(5x1=5)

1. Describe the different functions of Direct Memory Accesses (DMA) and its six steps Process to transfer data with suitable diagram.

- Used to avoid **programmed I/O** (one byte at a time) for large data movement
- Requires **DMA** controller
- Bypasses CPU to transfer data directly between I/O device and memory
- OS writes DMA command block into memory
  - Source and destination addresses
  - Read or write mode
  - Count of bytes
  - Writes location of command block to DMA controller
  - Bus mastering of DMA controller – grabs bus from CPU
  - When done, interrupts to signal completion



2. Write a detail notes about revocation of access rights in system protection

- Various options to remove the access right of a domain to an object
  - Immediate vs. delayed
  - Selective vs. general
  - Partial vs. total
  - Temporary vs. permanent
- Access List – Delete access rights from access list
  - Simple – search access list and remove entry
  - Immediate, general or selective, total or partial, permanent or temporary
- Capability List – Scheme required to locate capability in the system before capability can be revoked
  - Reacquisition – periodic delete, with require and denial if revoked
  - Back-pointers – set of pointers from each object to all capabilities of that object (Multics)
  - Indirection – capability points to global table entry which points to object – delete entry from global table, not selective (CAL)

- Keys – unique bits associated with capability, generated when capability created
  - Master key associated with object, key matches master key for access
  - Revocation – create new master key

Q3. Define the terms volume set, stripe set, and mirror set?

- **Volume set** is multiple disks that are logically concatenated to form a large logical volume.
- **Stripe set** is multiple physical partitions interleaved in round-robin fashion.
- **Mirror set** is two equally sized partitions on two disks with identical data contents.

Q4. What are the three techniques used for communicating data in a local procedure call?

Data is communicated using one of the following three facilities: 1) messages are simply copied from one process to the other, 2) a shared memory segment is created and messages simply contain a pointer into the shared memory segment, thereby avoiding copies between processes, 3) a process directly writes into the other process's virtual space.

Q5.Write any 4 categories of how security is violated?

Breach of confidentiality. This type of violation involves unauthorized reading of data (or theft of information). Typically, a breach of confidentiality is the goal of an intruder. Capturing secret data from a system or a data stream, such as credit-card information or identity information for identity theft, can result directly in money for the intruder.

• **Breach of integrity**. This violation involves unauthorized modification of data. Such attacks can, for example, result in passing of liability to an innocent party or modification of the source code of an important commercial application.

• **Breach of availability**. This violation involves unauthorized destruction of data. Some crackers would rather wreak havoc and gain status or bragging rights than gain financially. Website defacement is a common example of this type of security breach.

• **Theft of service**. This violation involves unauthorized use of resources. For example, an intruder (or intrusion program) may install a daemon on a system that acts as a file server.

- **Denial of service**. This violation involves preventing legitimate use of the system. **Denial-of-service (DOS)** attacks are sometimes accidental. The original Internet worm turned into a DOS attack when a bug failed to delay its rapid spread.

****